## AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. (Currently Amended) A method for protecting an embedded software, whereby a verification mechanism of the embedded software is modified as to require the embedded software to be operated in coordination with hardware characteristics of an authorized electronic information appliance~~, the electronic information appliance~~ having a storage device and firmware, the firmware arranging parameters of corresponding specific embedded software and providing a default parameter address, so as to enable execution of the embedded software corresponding to the firmware only in the authorized electronic information appliance, the method comprising the steps of:

(1) having a first program of the embedded software store parameters to be transmitted in a first address of the storage device, and having the embedded software pass a parameter access authorization through a function of the firmware to the firmware of the electronic information appliance;

(2) having the firmware rearrange ~~and store~~ the parameters to form rearranged parameters and store the rearranged parameters in a second address of the storage device, and handing over ~~the~~ an authorization of the rearranged parameters to the embedded software; and

(3) having the embedded software call and pass the authorization of the rearranged parameters to a second program of the embedded software, ~~and~~;

(4) having the second program extract and decode the parameters from ~~a default parameter~~the second address, to recovery initial contents of the parameters; and

(5) ~~determining~~ having the second program determine whether the rearranged parameters are correct, wherein, if the parameters are correct, enabling the execution of the embedded software ~~is properly executed, otherwise the embedded software is disabled~~in the electronic information appliance; if the parameters are not correct, prohibiting the execution of the embedded software in the electronic information appliance.

2. (Original) The method of claim 1, wherein the electronic information appliance is a storage server.

3. (Original) The method of claim 1, wherein the storage device is a memory.

4. (Original) The method of claim 1, wherein the firmware is a basic input/output system (BIOS).

5. (Original) The method of claim 1, wherein the first program is a main program of the embedded software.

6. (Original) The method of claim 1, wherein the address of the storage device in step (1) is a buffer in the memory.

7. (Original) The method of claim 1, wherein the function provided by the firmware is an appliance management interrupt (SMI) function.

8. (Currently Amended) The method of claim 1, further comprising encoding and rearranging ~~the~~ a sequence of the parameters before having the firmware rearrange and store the parameters according to a different sequence in a second address of the storage device in step (2).

9. (Original) The method of claim 1, wherein the second program is an auxiliary program of the embedded software.

10. (Currently Amended) The method of claim 1, wherein the embedded software is a storage management software.

11. (New) A method for protecting an embedded software from being copied and used without authorization, applying on an electronic information appliance comprising a RAM and a NVRAM, the method the comprising steps of:

receiving a quest with a plurality of parameters from a user to the embedded software;

storing the parameters to the RAM in a first type in a first address getting the parameters in a first type from the RAM;

changing the parameters to a second type and storing the parameters in the second type in the NVRAM; and

clearing the parameters in the RAM.

12. (New) The method of claim 11, wherein the embedded software executes the quest with the parameters by getting the parameters in the second type from the second address of the storage device.

13. (New) The method of claim 11, wherein the step of changing the parameters to the second type changes a sequence of the parameters.

14. (New) The method of claim 11, wherein the step of changing the parameters to the second type changes by coding a content of the parameters.

15. (New) The method of claim 11, wherein the storage device is a buffer in a memory.